Implementing Low-Power CRC-Half for RFID Circuits

Qi Mi, Zhi Li
ECE 632 – Fall 2008
University of Virginia
<qm8e, zl4s>@virginia.edu

ABSTRACT
RFID technology bridges the physical and virtual worlds by enabling computers to track objects of interest. However, without appropriate security protection, an attacker may be able to obtain secret information from the RFID tags. In this paper, we investigate the CRC-MAC scheme, which is suitable for encrypting data into hash values that are hard to decrypt without a correct key, and we implement its core function, i.e., CRC-Half, using PTM 90nm subthreshold technology. We also carry out extensive experiments to evaluate the performance of CRC-Half in terms of its energy consumption of CRC-Half. Experiment results show that an optimal supply voltage of 0.3V is desired.

1. INTRODUCTION
Radio-frequency identification (RFID) is an automatic identification method, relying on storing and remotely retrieving data using devices called RFID tags. The tags usually reply to a ready query by sending only an ID. Thanks to its convenience, the RFID technology has been widely used today in applications such as transportation and logistics, product tracking, animal identification, libraries, and inventory systems.

RFID tags usually come in the passive form. It does not have internal power supply. Therefore, many coils are used in the tags to couple the RF power that is propagated from the reader to produce enough voltage to operate the on-tag integrated circuit, as shown in Figure 1. Since the power an RFID tag can extract from the reader is limited, the circuit on the tag must be power-efficient and able to finish its processing and respond in a timely fashion. In addition to the power constraint, RFID tags need to be small and unobtrusive so that they can be easily attached to the objects of interest.

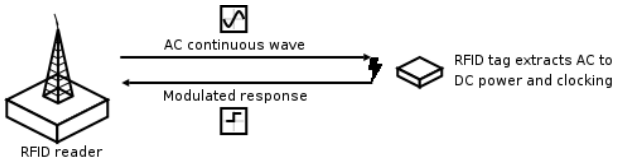


Figure 1. An RFID reader and an RFID tag

Widespread use of RFIDs has led to growing concerns about privacy and security, but the limited area and low power requirements on RFIDs prevent them from using traditional expensive cryptography [1]. Given the short reading time and the limited power that an RFID tag can absorb from the reader for it to process information and respond, a low-power implementation is highly desired.

In this project, we intend to make use of available reference and design a low-power implementation of CRC-Half. The rest of the paper is organized as follows: Section 2 lists some related work of RFID cryptography. Section 3 gives several design considerations. In Section 4, we present our simulation setup, results, and analysis. We conclude our work and propose some future work in Section 5.

2. RELATED WORK
Nowadays, most RFID applications do not have physical security protection mechanism. Therefore, the unsecured communication between an RFID reader and the tags may suffer from third-party eavesdropping, leaking important information. In [1], the authors identified private authentication as a key technical issue in library RFID applications where item-level tagging is required, i.e., how can a reader a tag that share a secret efficiently authenticate each other without revealing their identities to an adversary. To solve this issue, they provided a two-phase tree scheme with logarithmic communication for building private authentication.

In order to address the physical constraints of RFID tags, Nohl proposed CRC-MAC in [2]. Unlike traditional CRC functions which are highly linear and thus very susceptible to cryptographic attacks, CRC-MAC is an ultra lightweight strong keyed one-way function which is designed for security and privacy protocols. The design choices of the one-way hash function for CRC-MAC are limited in that the design has to fit on a very small device like an RFID tag. To meet this requirement, the author integrates the CRC function that is already found in a wide range of devices into CRC-MAC so that it can be implemented cheaply on resource-constrained devices.

3. IMPLEMENTING CRC-MAC
3.1 Design Goal and Assumptions
Our design goal is to implement CRC-MAC encryption operation with low energy consumption. Since the core encryption component of CRC-MAC is CRC-Half, we will focus on designing low-power CRC-Half circuit that can compute the desired encrypted hash value correctly within reasonable time duration.

For simplicity, we assume that the coils in the RFID tag have already coupled sufficient energy from an external device and can thus provide stable power supply V_{DD} for CRC-MAC operation.

3.2 Logic Design
Figure 2 provides a C implementation of CRC-MAC. As shown, CRC-MAC works by taking in several data words and key words, executing CRC-Half (which is a modified CRC) to compute a hash value for a given data word, and then updating this data word in the data register. Accordingly, our schematic of CRC-Half will include a circuit-enable component, a signal-control component, a polynomial generator component, and a hash loop component.

```
// compute generator polynomial and
// execute the 16-bit CRC function on state s for 8 clock cycles
u16 CRC_half(u16 s, u16 k)  // s := CRC state, k:= key input
{
    u16 g,j;
    // compute generator from half of data word and key input and
    // set highest bit of generator to '1'
    g = ( s & 0xFF )^( k | ( 0x8000 ));
    // shift for 8 clock cycles and
    // XOR state with generator when lowest state bit is '1'
    for( j = 0; j<8; j++)
        s = ( s & 1 ) ? ( s>>1 )^g : ( s>>1 );
    return s;
}

// compute 16-bit CRC-MAC, hash output is left in x[]
CRC-MAC(u16* key, int n_key     // key  :  key[n_key]
        u16* x,   int n_data)   // state:  x[n_data]
{
    u16 r;
    for ( r = 0; r < 4*(3*n_data+n_key); r++)
    {
        x[r%n_data] ^= ~r;
        CRC_half(x[r%n_data],
                 key[r%n_key] ^ x[(r+1)%n_data] ^
                 (n_data>2 ? x[(r+n_data-1)%n_data] : 0));
    }
}
```

Figure 2. C implementation of CRC-MAC

3.3 VLSI Design Choice

3.3.1 CMOS

Ratioed logic and passgate-based logic might seem to be appealing design candidates because either of them would require few transistors than their CMOS counterpart. Nonetheless, they either suffer from static leakage or reduced output swing. On the contrary, CMOS implementation has the advantages of little static leakage and full output swing. Furthermore, CMOS has proved to have quite large noise margins in sub-threshold technology. Given these favorable characteristics of CMOS, we will use the CMOS design.

3.3.2 Minimum Sizing

In [3], B. Calhoun *et al* have examined the effect of sizing on energy consumption for subthreshold circuits. They have also shown that minimum sized devices are theoretically optimal for reducing energy. We will use minimum-sizing for all transistors unless their fan-out exceeds four.

3.3.3 Subthreshold Voltage

Subthreshold operation has become an emerging technology for low-power circuit design, where the operation delay is not a crucial factor.

For a general circuit,

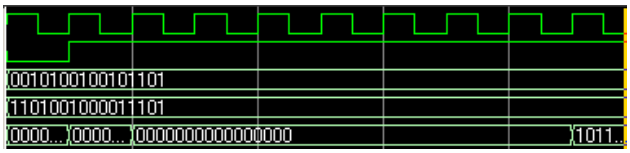
$$E/op = E_{\text{active}} + E_{\text{leakage}} = C_{\text{eff}} V_{\text{DD}}^2 + I_{\text{lkg}} V_{\text{DD}} T_{\text{D}} \qquad (1)$$

where C_{eff} is the total equivalent lumped capacitance and T_{D} is the delay to complete the entire operation. As suggested by (1), E_{active} is proportional to the square of V_{DD}. Therefore, when V_{DD} goes down, E_{active} will decrease substantially. However, an adverse effect of lowering V_{DD} is the introduction of considerably longer operation delay T_{D}, resulting in an increased leakage energy E_{lkg}. Since E_{lkg} will become a dominant portion of the total energy as V_{DD} scales down, we must carefully analyze a specific VLSI circuit and find its optimal supply voltage at which its total energy consumption is minimal.

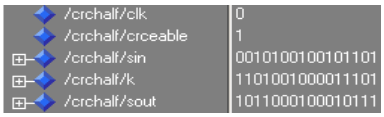
4. SIMULATION

4.1 Simulation Setup

We first designed the CRC-Half circuit using FPGA Advantage 7.0 LS and simulated its logic. In this circuit, 16-bit data words and 16-bit key word are input at the beginning of a processing. After 10 clock cycles, the hashed value is ready to output. An example output is shown in Figure 3.



(a)



(b)

Figure3 (a) Waveform of CRC_Half circuit (b) Final values of variables.

This circuit has been tested for various random inputs and the logic results matched with the C program.

Then we built the whole circuit using netlists in Cadence: We first employed the 90nm PTM model in our circuit to ensure a high operation speed. We built a library file describing all the gates and registers needed for the CRC circuit with PTM 90nm technology, then four CRC-Half components, together with basic gates and registers and the whole circuit at last. The circuit has been simulated in Cadence and the result was correct. A sample output of updated data word is shown in Figure 4.

4.2 Metric

We use the total energy consumption of a CRC-Half processing as our metric. We try to come to a design that minimizes this metric.

4.3 Average Current Measurement

We have tried to simulate the power by averaging the current going through V_{DD} . The circuit setup is shown in Figure 5.

We evaluated the average total current going through V_{DD} at different CLK frequencies and at different V_{DD} in a complete CRC-Half operation. We also evaluated the leakage current, given fixed inputs and non-changing CLK.

4.4 Results and Discussion

4.4.1 Leakage Current

Subthreshold leakage current is the drain to source current when the transistor is in the "off" (or weak inversion) condition. This happens when the gate-to-source voltage V_{GS} is less than the threshold voltage V_{T}[5, 6]. The current in the weak inversion region can be approximated by the following expression:

$$I_D = I_o \left(\frac{W}{L}\right) 10^{\frac{V_{GS}-V_T+\eta V_{DS}}{s}} \left(1 - e^{-\frac{V_{DS}}{V_{th}}}\right) \qquad \textbf{(2)}$$

From the simulation result of the leakage current of CRC-Half, we found that as long as the CLK cycle is long enough for proper circuit operation (charging and discharging), the leakage current

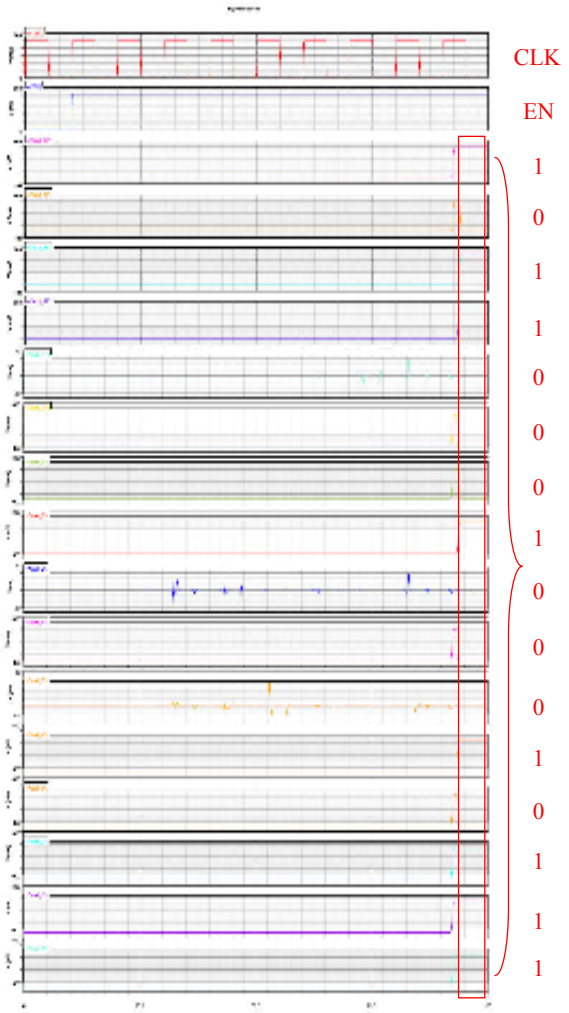


Figure 4. The waveform of the output during a processing cycle. CRC-Half output is produced in the last CLK cycle

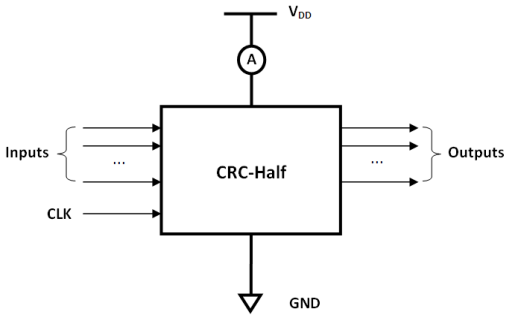


Figure 5. Drain-source current measurement setup

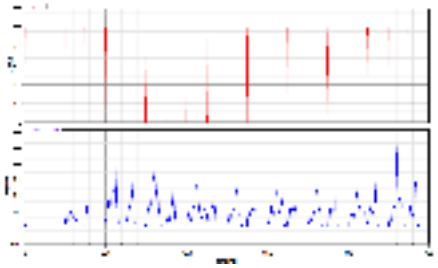


Figure 6. A sample waveform of transient current in CRC-Half

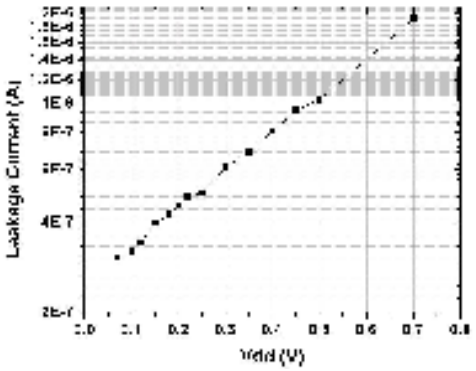


Figure 7. log(I_{lkg}) vs V_{DD} curve

remained almost the same for any certain V_{DD} no matter how fast the CLK rate was (see Figure 6). A leakage current vs. V_{DD} plot is shown in Figure 7. Note that the Y axis of this figure is plotted in the logarithmic scale and this curve looks pretty much like linear. In fact, this result can be well explained by (2). Due to the DIBL effect, a transistor's leakage current is exponentially dependent on V_{DS}. Since V_{DS} is approximately proportional to the power supply V_{DD}, the logarithmic value of leakage current is approximately proportional to V_{DD}. Thus, our result is consistent with the DIBL theory.

4.4.2 Energy Consumption & Optimal Supply Voltage

Given a certain V_{DD}, we gradually increase the clock frequency to f_{cr} (or equivalently, decrease the clock period to T_{cr}) until the output logic of CRC-Half starts to fail. We obtain the average current for this operation, $I_{avg,}$, at this supply voltage. Then,

$$E_{total} = V_{DD} I_{avg} n_{CRC\text{-}Half} / f_{cr} \quad (3)$$

where $n_{CRC\text{-}Half} = 9$ is the number of clock cycles to complete a CRC-Half operation.

As discussed in 4.3.2, assume that under a certain power supply, the power consumed in each CLK cycle is approximately the same. In the mean while, leakage current only depends on the voltage supply, which means a faster CLK rate would actually help reduce energy consumption in one CRC-Half processing cycle.

For a certain V_{DD}, we have run CRC-Half with Ocean at different CLK rates, and found out the slowest CLK rate at which the circuit failed and the fastest CLK rate at which the circuit still worked properly. We also recorded the average current corresponding to the fastest CLK rate and calculated the total energy consumption. The simulation data is given in Table 1.

Similarly, given a certain V_{DD} and corresponding critical clock frequency f_{cr}, we measure the total leakage current I_{lkg} of the CRC-Half circuit when the circuit is idle, and compute leakage energy corresponding to following formula.

$$E_{lkg} = V_{DD} I_{lkg} n_{CRC\text{-}Half} / f_{cr} \quad (4)$$

Table 1. Total energy consumption at different supply voltages

V_{DD} (V)	T_{cr} (ns)	I_{avg} (A)	E_{total} (nJ)
0.5	10	3.09E-05	1.55E-03
0.45	15	1.98E-05	1.33E-03
0.4	20	1.33E-05	1.06E-03
0.35	40	6.20E-06	8.68E-04
0.3	70	3.50E-06	7.36E-04
0.25	200	1.53E-06	7.63E-04
0.2	700	7.16E-07	1.00E-03
0.15	1800	4.84E-07	1.31E-03

Table 2. Leakage energy consumption at different supply voltages

V_{DD} (V)	T_{cr} (ns)	I_{lkg} (A)	E_{lkg} (nJ)
0.5	10	1.03E-06	5.15E-05
0.45	15	9.48E-07	6.40E-05
0.4	20	8.07E-07	6.46E-05
0.35	40	6.87E-07	9.62E-05
0.3	70	6.11E-07	1.28E-04
0.25	200	5.03E-07	2.52E-04
0.2	700	4.55E-07	6.37E-04
0.15	1800	3.97E-07	1.07E-03

The total energy consumption and the leakage energy consumption for CRC-Half are plotted in Figure 8. We also subtract the E_{lkg} from E_{total} to obtain the active energy consumption E_{active} and plot it on the same figure. Note that E_{total}, E_{lkg}, and E_{active} are all measured within one CRC-Half processing.

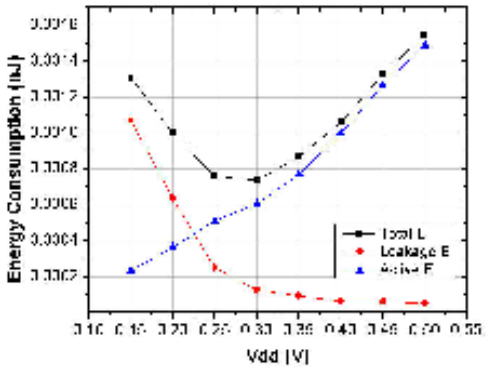


Figure 8. Energy consumption vs V_{DD} curves for CRC-Half

From Figure 8, we can tell that the optimal supply voltage is 0.3V in the subthreshold region, corresponding to a CLK rate about $1/(70*10^{-9})$=14.3MHz. The corresponding minimum energy consumption that we can achieve is 0.736 pJ.

4.4.3 Discussion

According to $P_{avg} = \alpha_{0\to1} f C_{eff} V_{DD}^2$, dynamic power is proportional to the clock frequency of the circuit. Therefore, it seems like we could try to turn down the clock frequency (or equivalently, increase the clock period) in order to reduce the dynamic power drawn from the power supply. However, for a circuit that operates in the subthreshold region, its leakage current is dominant. Therefore, an increased clock period would contribute to an increased leakage power. So rather than reducing the CLK rate, speeding up the circuit till the logic almost fails might actually help save energy.

Besides, using two or multiple power supplies might help to speed up the circuit to reduce leakage energy. Using higher voltage supply in the slow parts of the whole circuit while keeping low voltage supply for remaining parts to provide a better delay balance should really help speed up the circuit, and therefore reducing energy consumption. Similarly, sizing up some slow part of the circuit would also help reduce energy for the same reason.

Furthermore, we can see from our simulation that in the sub-threshold operation region of 90nm-technology, the leakage current is taking up a large proportion of the average total current. And the energy consumed by leakage current is quite comparable or even larger than active energy. The situation might be even worse in the state of the art technology such as the 65nm technology used in the Intel Duo Core processor and the 45nm technology used in the Intel Atom Processor. An effective way to reduce the leakage problem is to use high V_T transistors to limit the leakage current when the circuit is idle. Although this method does not suit our RFID design (since real RFID tags do not have internal power supply), it is still quite worthy in other RF-controlled devices.

5. CONCLUSION

CRC-Half, the core of CRC-MAC, has been implemented and simulated in FPGA and Cadence. The average and leakage currents were simulated and different energy consumptions were compared at different voltage supplies. The optimal supply voltage was found to be at around 0.3V with the minimum energy consumption of 0.736pJ/operation. Based on the simulation, some methods are proposed to further reduce energy consumption.

6. ACKNOWLEDGMENTS

The authors would like to thank to Professor Benton Calhoun for his valuable advice on this project. The authors would also like to thank Jiajing Wang and Jiawei Huang for their kind discussion.

7. REFERENCES

[1] Molnar, D. and Wagner, D. Privacy and Security in Library RFID: Issues, Practices, and Architectures ACM CCS, 2004.

[2] Nohl, K., *Implementable Privacy for RFID Systems*, PhD Dissertation, Department of Computer Science, University of Virginia, 2008.

[3] Calhoun, B., Wang, A., Chandrakasan, A. *Modeling and Sizing for Minimum Energy Operation in Subthreshold Circuits*, IEEE Journal of Solid-State Circuits, vol. 40, No. 9, September 2005, 1778-1786

[4] Calhoun, B., Chandrakasan, A. *Ultra-Dynamic Voltage Scaling Using Sub-Threshold Operation and Logical Voltage Dithering*, IEEE International Solid-State Circuits Conference, February 2005, 300-301

[5] Deepak, B., Nunez, A., *Analysis of Subthreshold Leakage Reduction in CMOS Digital Circuits*, Proceedings of the 13th NASA VLSI Symposium, June, 2007

[6] Rabaey, J., Chandrakasan, A., Nikolic, B., *Digital Integrated Circuits, A Design Perspective, 2nd Ed*, Prentice Hall, 2002.

[7] Cadence Design Systems, *Virtuoso® Spectre Circuit Simulator User Guide v 7.0.1*, June, 2008

[8] Cadence Design Systems, *OCEAN Reference v 5.1.41*, July, 2007.